REMARKS

Applicants would like to thank the Examiner for the thorough examination of the present application, and for withdrawing the claim rejections over the published patent application to Luyster.

The independent claims have been amended to more clearly define the present invention over the cited prior art references. Certain dependent claims have been cancelled and others have been amended for consistency. The claim amendments and arguments supporting patentability of the claims are provided below.

I. The Claimed Invention

The present invention, as recited in independent Claim 1, for example, is directed to a cryptographic device comprising an input stage, and an intermediate stage connected to the input stage. The input stage receives an input data block and a key data block comprising a plurality of sub-key data blocks, and generates a plurality of first signals therefrom that are in parallel. The intermediate stage comprises a plurality of substitution units operating in parallel, each substituting data within a respective first signal. A diffuser is connected to the plurality of substitution units for mixing data to generate a diffused signal. The diffuser comprises at least one shift register and at least one look-up table associated therewith. An output stage is connected to the intermediate stage for repetitively looping back the diffused signal to the input stage for combination with a next sub-key data block.

Independent Claim 10 is directed to a communication system comprising a key scheduler and a cryptographic device connected to the key scheduler, and has been amended similar to amended independent Claim 1.

Independent Claim 18 is directed to a method for converting an input data block into an output signal in a cryptographic device, and has been amended similar to amended independent Claim 1.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 10 and 18 over the Kanda et al. patent. Independent Claims 1, 10 and 18 have been amended to include the subject matter from their respective dependent Claims 5, 13 and 22. The rejections of the claims will still be discussed in view of the Kanda et al patent. Kanda et al. is directed to a data transformation device for use in an encryption device of a secret key encryption algorithm that encrypts or decrypts data blocks using a secret key.

The Examiner referenced FIGS. 1, 2, 4 and 5 in Kanda et al. as disclosing the claimed invention. The Examiner characterized the input stage **17** as illustrated in FIG. 2 as generating a plurality of first signals that are in parallel. The intermediate stage comprises a plurality of substitution units (S-boxes S_0-S_7) operating in parallel, each substituting data within a respective first signal. The Examiner also characterized block **346** as a diffuser connected to the plurality of substitution units S_0-S_7 for mixing data to generate a diffused signal.

The amended independent claims recite that an output stage is connected to the intermediate stage for repetitively looping back the diffused signal to the input stage for combination with a next sub-key data block. The Examiner has characterized that the round processing **38_0-38_{N-1}** in Kanda et al. each provides an output to the next one of the processing parts for combining with another subkey data block. The Examiner has characterized that the round processing **38_0-38_{N-1}** corresponds to the repetitively looping back in the claimed invention.

With respect to the diffuser comprising at least one shift register and at least one look-up table associated therewith, the Examiner referenced column 13, line 63 to column 14, line 28. The Examiner states that the logical linear operations in Kanda et al. correspond to the shift registers in the claimed invention. Portions of column 13, line 63 to column 14, line 28 in Kanda et al. are as follows:

> "The outputs from the XOR circuits **32_0**, **32_1**, **31_2** and **31_3** and subkey data k_{i10}, k_{i11}, k_{i12} and k_{i13} are XORed by XOR circuits **35_0** to **35_3** of the key-dependent transformation part **344B**, respectively, from which are provided mid_{10}, mid_{11}, mid_{12} and mid_{13}. In other words, the pieces of data mid_{00}, mid_{01}, mid_{02} and mid_{03} are associated with one another and then undergo linear transformation dependent on the 8-bit subkey data k_{i10}, k_{i11}, k_{i12} and k_{i13}, respectively." (Emphasis added).
>
> "As depicted in FIG. 5, these pieces of data mid_{10}, mid_{11}, mid_{12} and mid_{13} are then nonlinearly transformed in the nonlinear transformation parts **345_0**, **345_1**, **345_2** and **345_3**

> into the data out_0, out_1, out_2 and out_3, respectively, which are combined into the single piece of data Y_i* in the combining part **346**." (Emphasis added).

As noted above, the Examiner is now characterizing the second key linear transformation part **344** as the diffuser. Before, the Examiner characterized block **346** as the diffuser.

In reference to the second key linear transformation part **344**, the second key linear transformation part **344** includes a linear transformation part **344A**, and a key-dependent linear transformation part **344B** that has been added to the linear transformation part **344A**, as illustrated in FIG. 7. Both of these sections comprise a plurality of XORs.

In sharp contrast, the amended independent claims recite that the diffuser comprises at least one shift register and at least one look-up table associated therewith. In Kanada et al., even if the Examiner characterizes the logical linear operations in Kanda et al. as corresponding to the shift registers, there is simply no reference to a look-up table as in the claimed invention.

Kanada et al. discloses other embodiments of the second key linear transformation part **344** in FIGS. 16-19 and 21, for example. In each of these embodiments, there is no reference to a look-up table associated with a shift register. Again, a plurality of XORs is connected together. Even block **346** previously indicated by the Examiner as being a diffuser fails to disclose a look-up table. Instead, the combining part **346**

receives the outputs from the second key linear transformation part **344** and generates a single output.

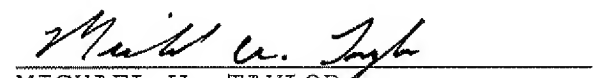
Accordingly, it is submitted that amended independent Claim 1 is patentable over Kanda et al. Amended independent Claims 10 and 18 are similar to amended independent Claim 1. Therefore, it is submitted that these claims are also patentable over Kanda et al.

In view of the patentability of amended independent Claims 1, 10 and 18, it is submitted that the dependent claims, which include yet further distinguishing features of the invention are also patentable. These dependent claims need no further discussion herein.

III. CONCLUSION

In view of the claim amendments and arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



MICHAEL W. TAYLOR
Reg. No. 43,182

In re Patent Application of:
KURDZIEL ET AL.
Serial No. **10/780,848**
Confirmation No. **2513**
Filed: **FEBRUARY 18, 2004**
_____/

Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330